Features and usage examples of wAP device

Maris Bulans
MikroTik, Latvia

MUM Mongolia
June 2017

Features and usage examples of wAP device

Maris Bulans
MikroTik, Latvia

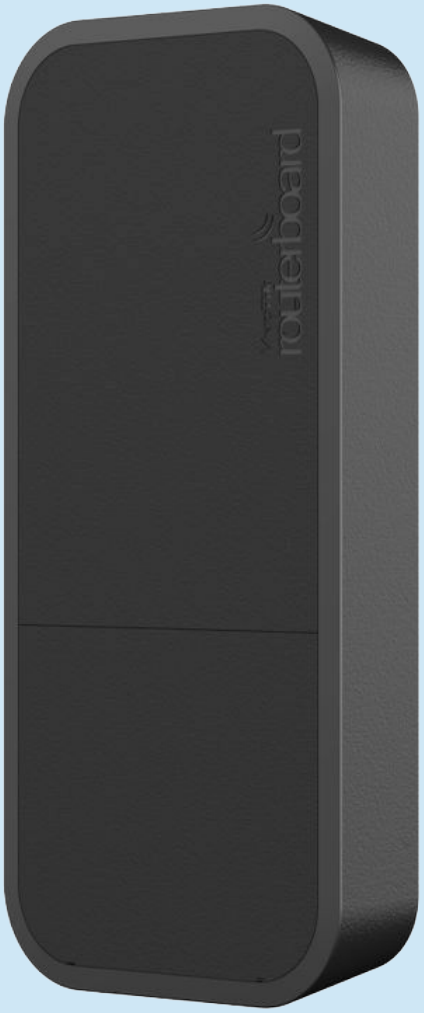
MUM Mongolia
June 2017

Overview

- Gift from MikroTik – wAP
- Repeater Setup
- CAPsMAN overview and basic config

wAP

Black and White edition



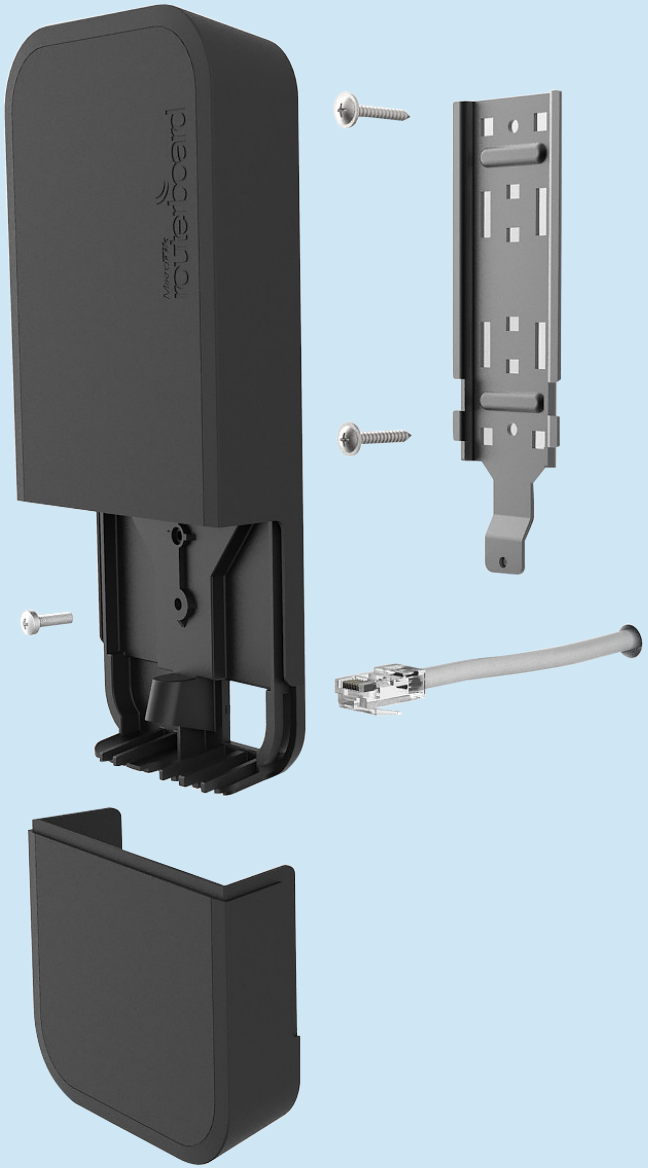
Features

- CPU 650 MHz
- RAM 64 MB
- Flash 16 MB
- Wireless 802.11b/g/n dual-chain
- Gain 2dBi antennas
- Ethernet 10/100Mbps
- Dimensions 185 x 85 x 30 mm

Features cont

- Wide input Voltage (11-57V)
- 802.3af/at, Passive PoE and power jack
- Low Power Consumption (up to 4W)
- High Operating Temp (-40C to +70C)
- Weatherproof case design suitable for indoor and outdoor

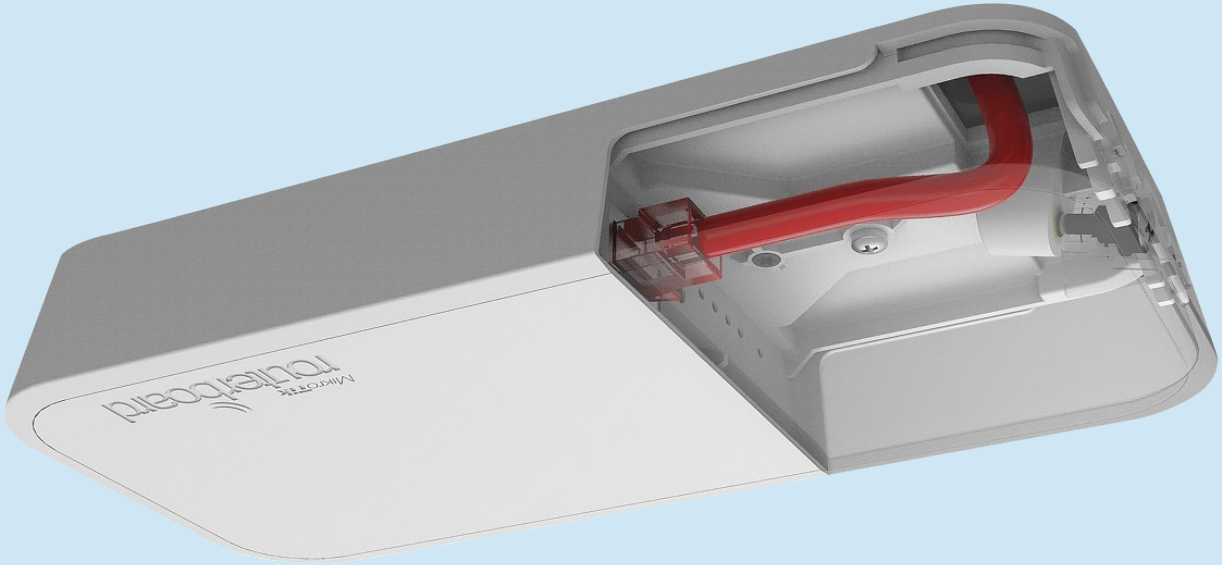
Usage Cases



Use it on the wall!

- Wall mounting is easy thanks to the provided drill template and screw anchor. Everything included

Usage Cases



Use it on the ceiling!

- The WAP comes bundled with all the necessary things to be mounted on ceiling
- Cable breakout provides ability to run cable through the ceiling

Default Configuration

- Ether1 configured as WAN port
  - Firewall protection (only ping allowed)
  - Masquerade enabled
  - DHCP client enabled
  - Neighbour discovery disabled
- Fast-track enabled
- Default local IP: 192.168.88.1/24
- Wireless access point enabled
- SSID: MikroTik-<last 6 chars from MAC>
- DHCP server on wireless AP

How to Connect

Ethernet (WAN) port is protected

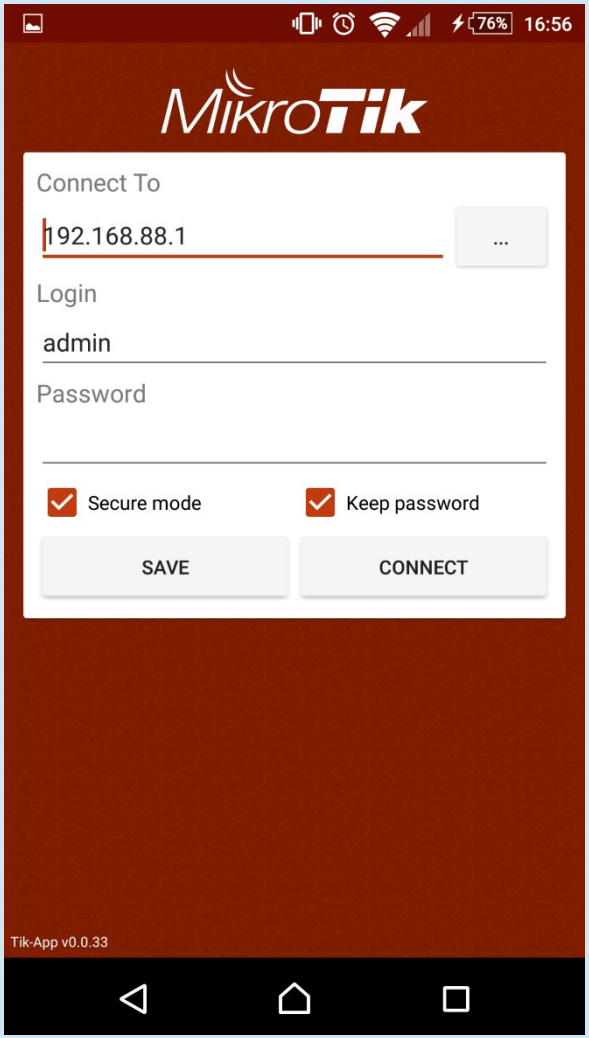
- Connect laptop to wireless and use Winbox/WebFig, telnet or ssh
- Connect android phone to wireless and use TikApp or WebFig
- Default IP address 192.168.88.1
- Default username: admin w/o password

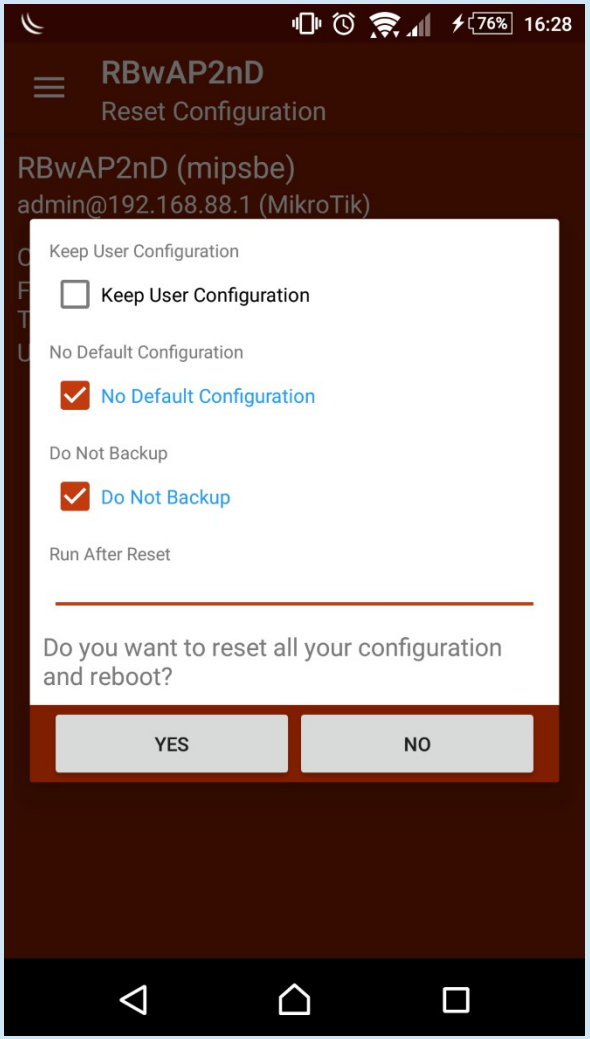
Default configuration can be switched to CAP mode by holding reset button for 10 seconds.

- Wireless and ethernet bridged
- DHCP client enabled on bridge interface

TikApp

- Sign to testing program, link on Mikrotik forum
- Download TikApp in Play store





Secure the Router

- Connect and set username/password
- Disable ‘admin’ user
- Set WPA and WPA2 key to secure AP

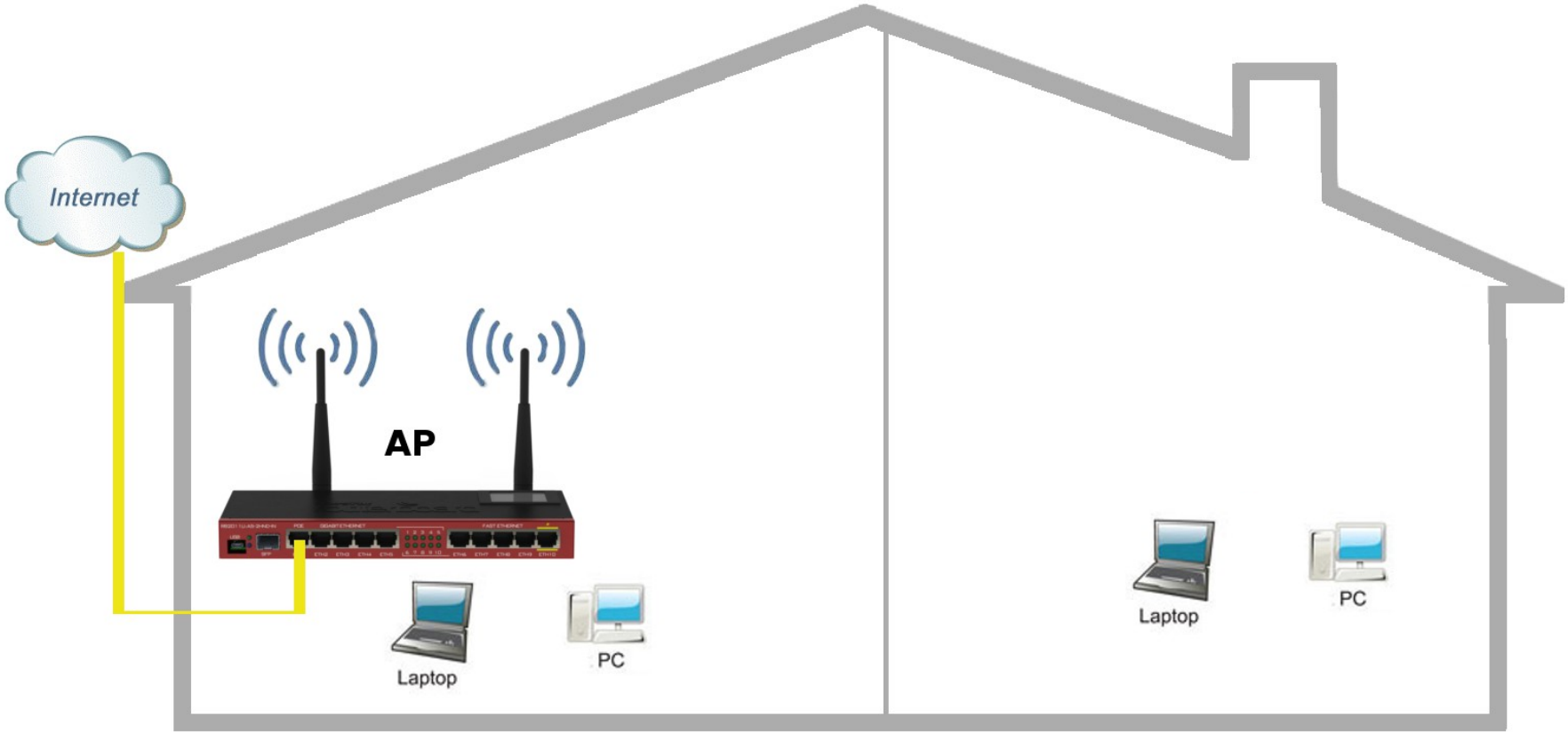
Repeater at Home

Routers have great coverage, but consumer devices (laptops, mobile phones, refrigirators, toilet seats) does not.

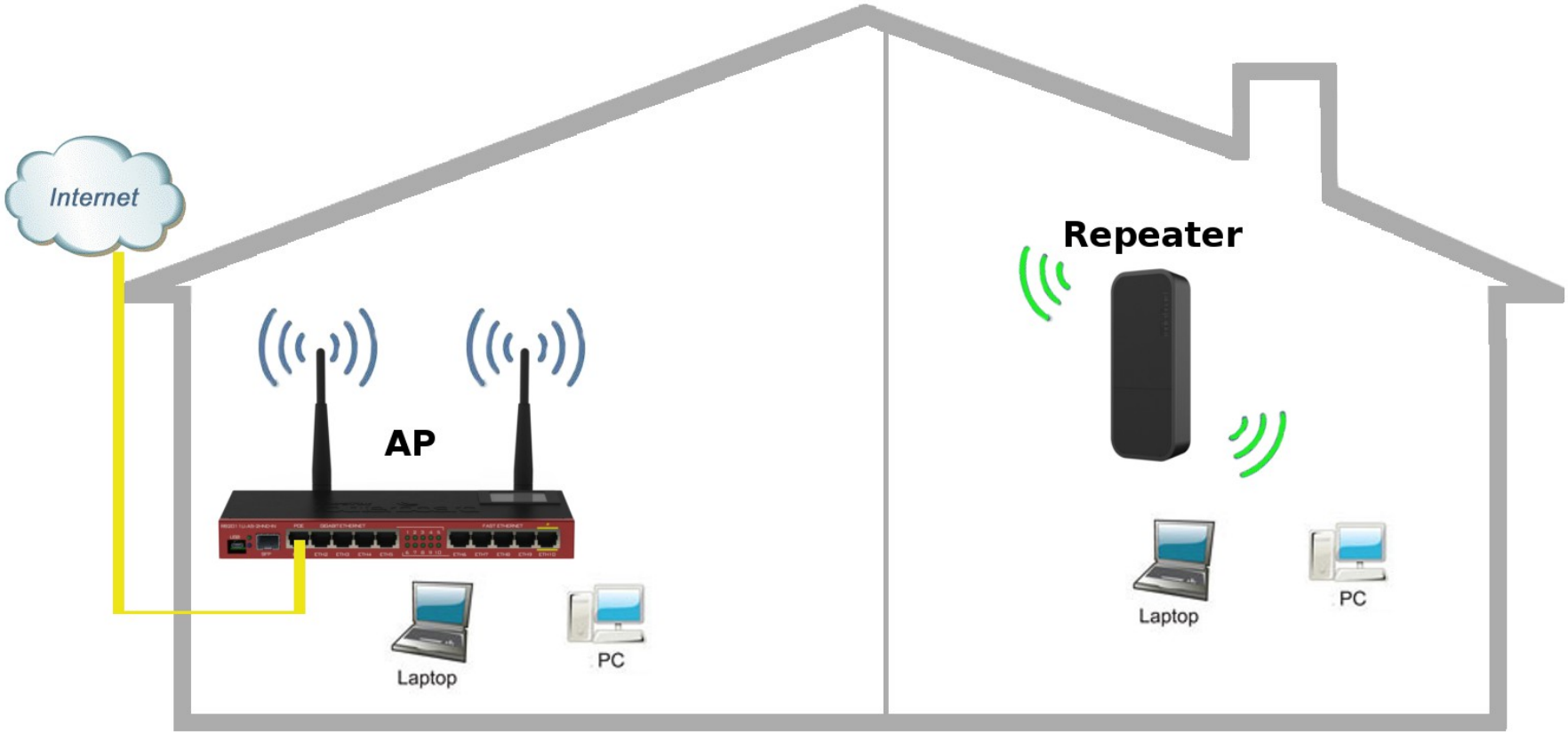
Wireless repeaters extend your wireless network range without requiring you to add any wiring.

Repeater should have two wireless interfaces or set up virtual AP.

Repeater at Home



Repeater at Home



Repeater Setup

Configure wireless settings manually to connect to MikroTik access point:

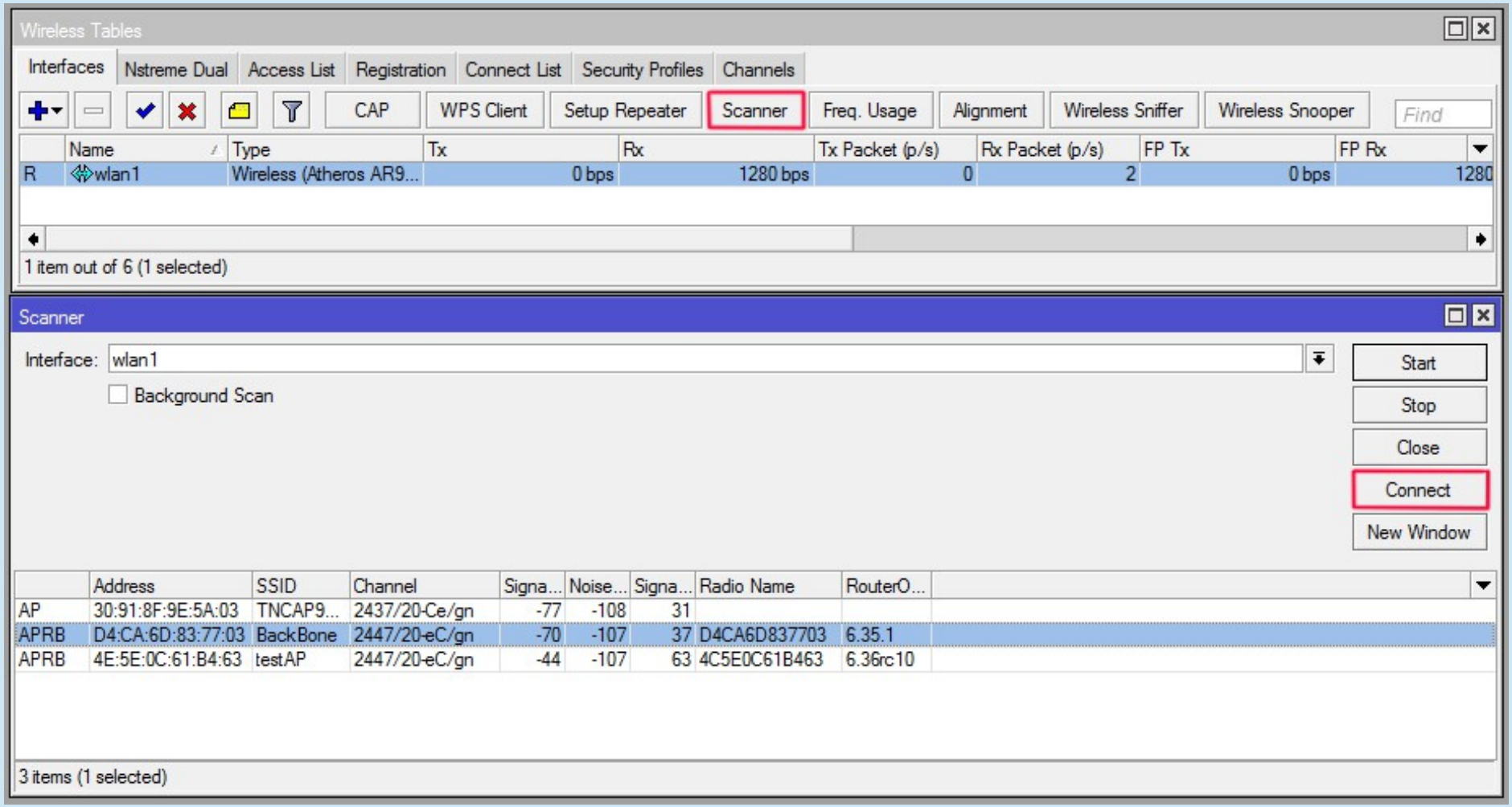
- Configure security profiles (authentication-type, mode, key)
- Configure wireless settings (station mode,band, SSID)

For repeater setups station mode should be “station-bridge” (works only with MT APs).

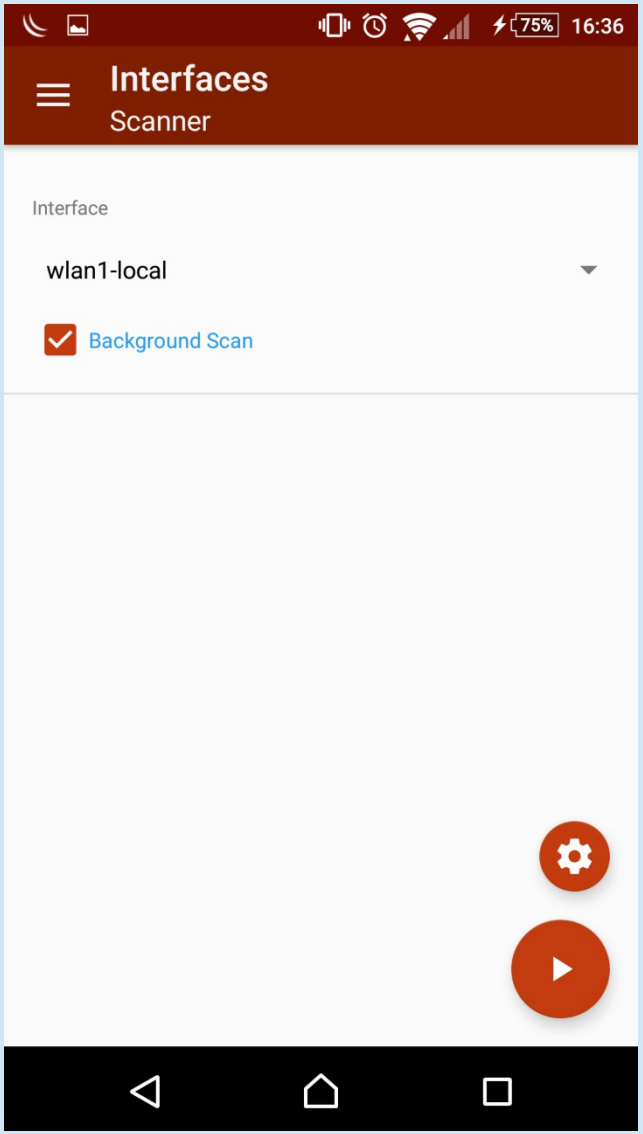
Or use wireless scan feature.

Wireless Scan

Fastest way to connect to AP



TikApp Scan


75% 16:36
Interfaces
Scanner
Interface
wlan1-local
Background Scan

75% 16:35
Interfaces
Running
Interface: wlan1-local
Address: D4:CA:6D:FA:FE:40
SSID: r201
Channel: 2412/20/g
Signal Strength: -64
Noise Floor: 0
Signal To Noise: 0
Radio Name: D4CA6DFAFE40
RouterOS Version: 6.36rc18
Interface: wlan1-local
Address: D4:CA:6D:B0:E1:B5
SSID: ez_2011UAS
Channel: 2412/20/g
Signal Strength: -41
Noise Floor: 0
Signal To Noise: 0
Radio Name: D4CA6DB0E1B5
RouterOS Version: 6.36rc18
Interface: wlan1-local
Address: D4:CA:6D:A2:7E:D4
SSID: Anrijs-2011
Channel: 2412/20/g
Signal Strength: -69
Noise Floor: 0
Signal To Noise: 0
Radio Name: D4CA6DA27ED4
RouterOS Version: 6.99
Interface: wlan1-local
Address: E4:8D:8C:49:3D:B2
SSID: MT-CAP
Channel: 2412/20-Ce/gn

Background Scan

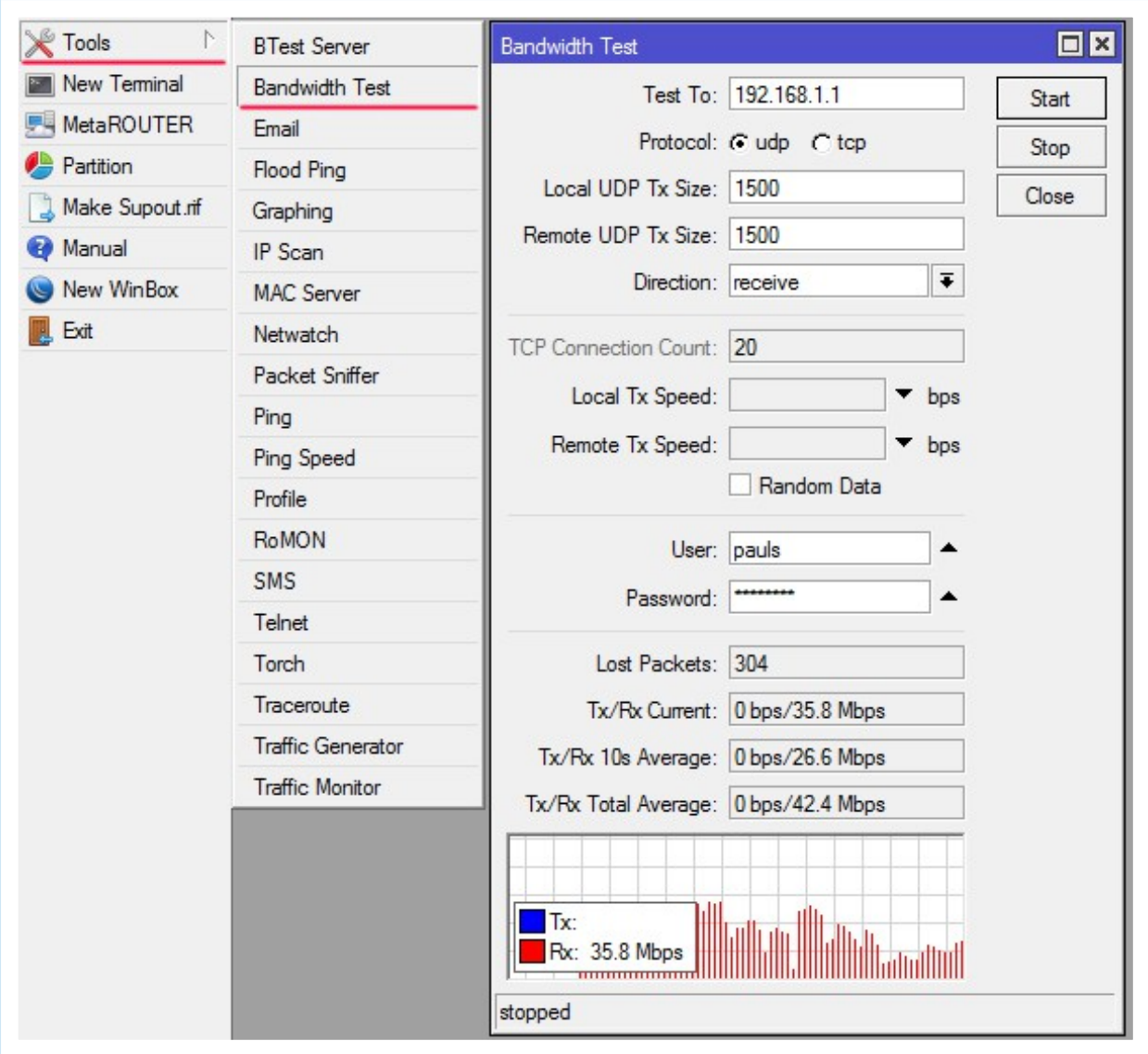
- Supported for 802.11 protocol only
- Working conditions
  - Wireless interface should be enabled
  - For AP mode – when operating on fixed channel
  - For Station mode – when connected to AP
- Supported also on Virtual interfaces
  - Scan is only performed in channel where master interface is running
- Allows to save the scan results in a CSV format file

Repeater Setup

- Add virtual AP interface
- Use the same SSID and security settings
- Add bridge interface with static MAC address
- Bridge physical wireless interface with virtual AP
- Add DHCP client on bridge interface for management(optionally)

Test troughput

Measure troughput between wireless devices



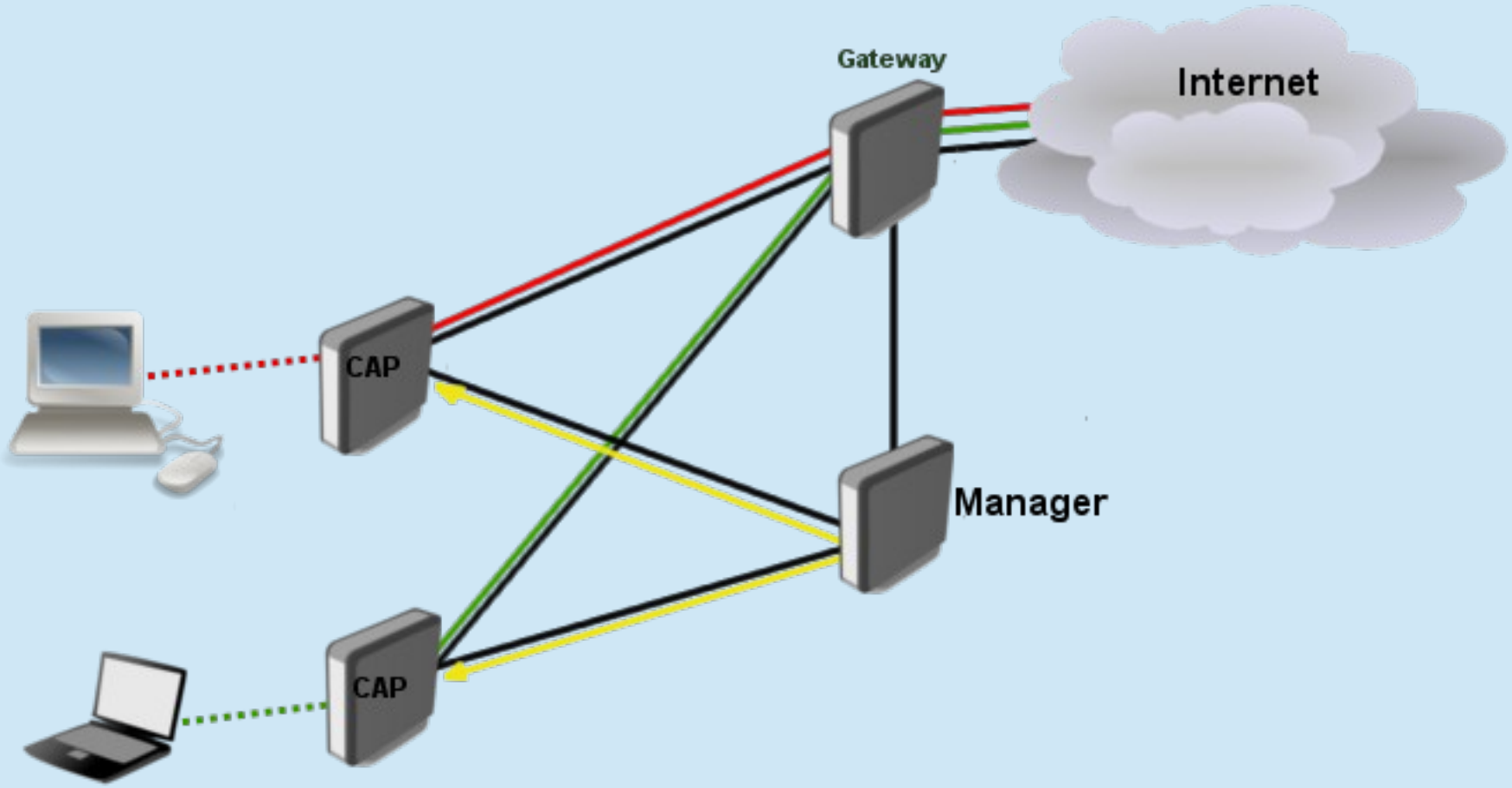
WPS Client Support

- Allows wireless client to get Pre-Shared Key configuration of the AP that has WPS Server enabled
- Gets information from any WPS Server running or can be specified to get only with specific SSID or MAC address
- Received configuration is shown on the screen and can be also saved to a new wireless security profile

CAPsMAN

- Controlled Access Point system Manager (CAPsMAN)
- Network consists of a number of 'Controlled Access Points' (CAP)
- CAP requires almost no configuration
  - connectivity to CAPsMAN (IP or MAC)
  - wireless lock to capsman
- Packet processing:
  - central (default),
  - local forwarding.

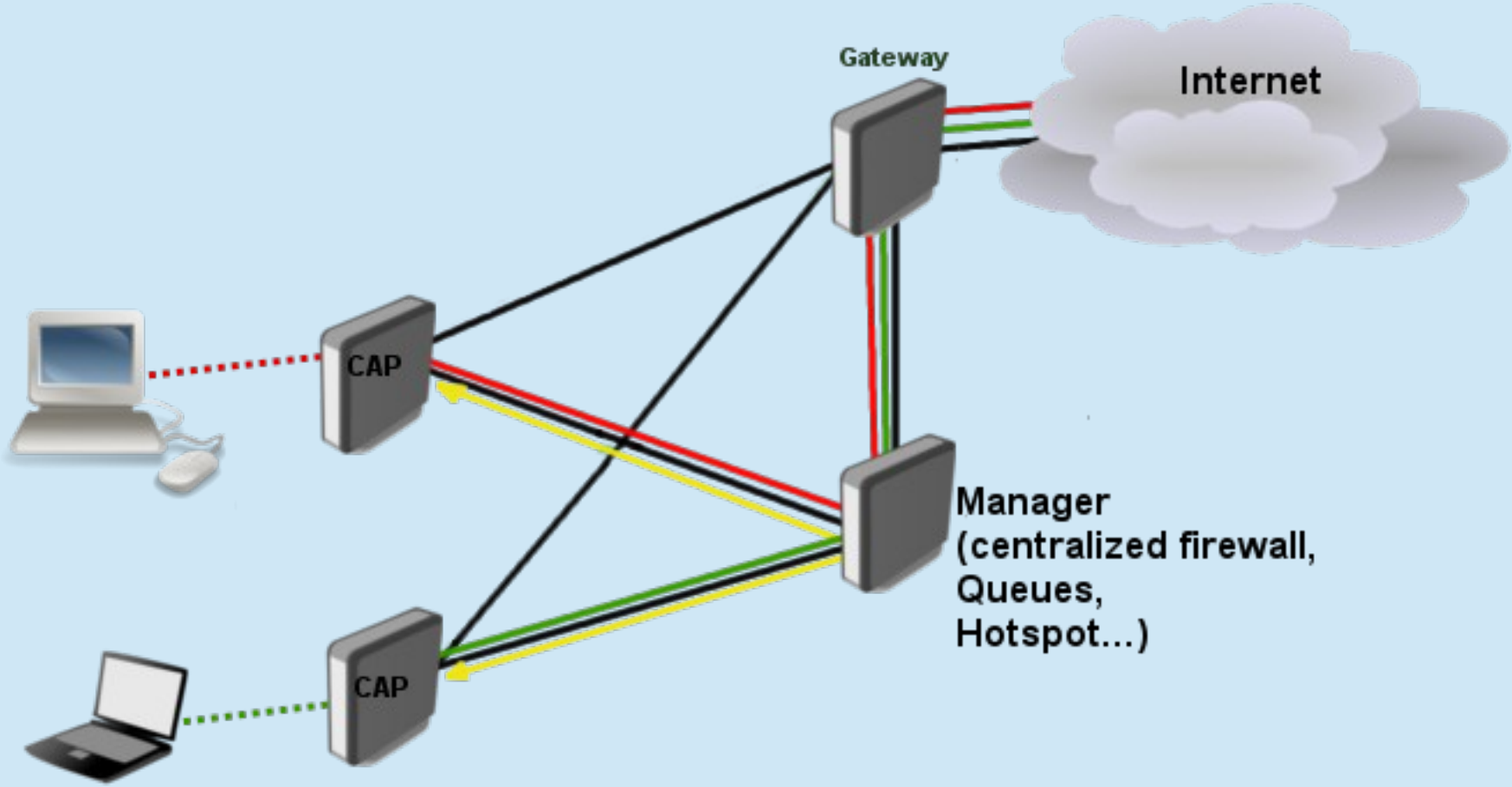
Local Forwarding



Local Forwarding

- Pros:
  - Manager can be router with weak CPU
  - Link between manager and gateway not so important
  - Clients do not loose connectivity to internet after CAPsMAN failure
- Cons:
  - Not so friendly for central management
  - Hotspot, firewall, queues, DHCP server in most cases handled locally by CAPs

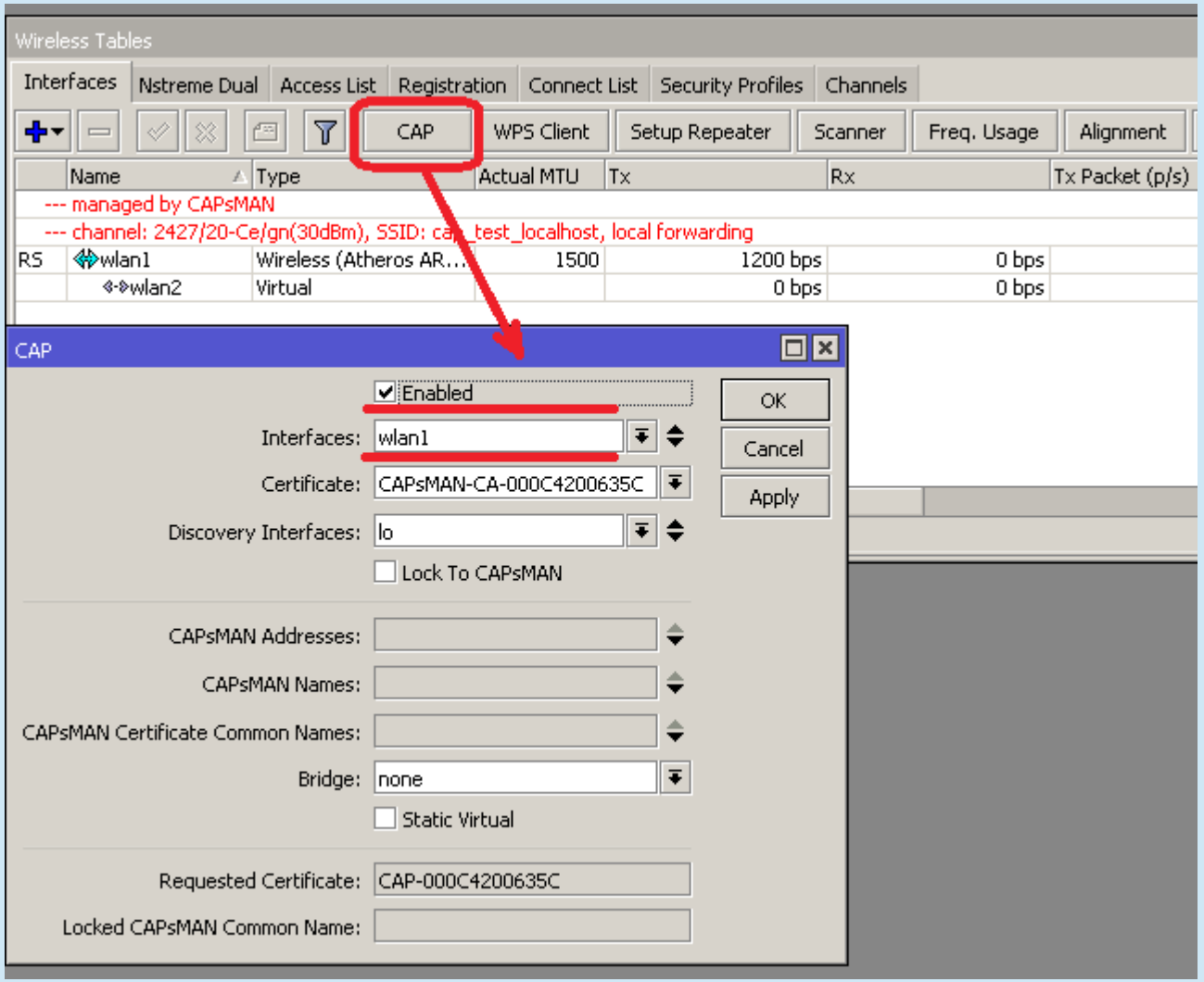
Central Forwarding



Central Forwarding

- Pros:
  - Easy service management on single router
  - Hotspots, DHCP servers, firewall etc can be controlled by groups on single machine
- Cons:
  - Single point of failure (backup CAPsMAN can be set)
  - Hardware must be powerful with fast CPU
  - Link between Manager and Gateway must be stable and fast.

CAP Configuration



CAP Configuration

```
/interface wireless cap set enabled=yes interfaces=wlan1
```

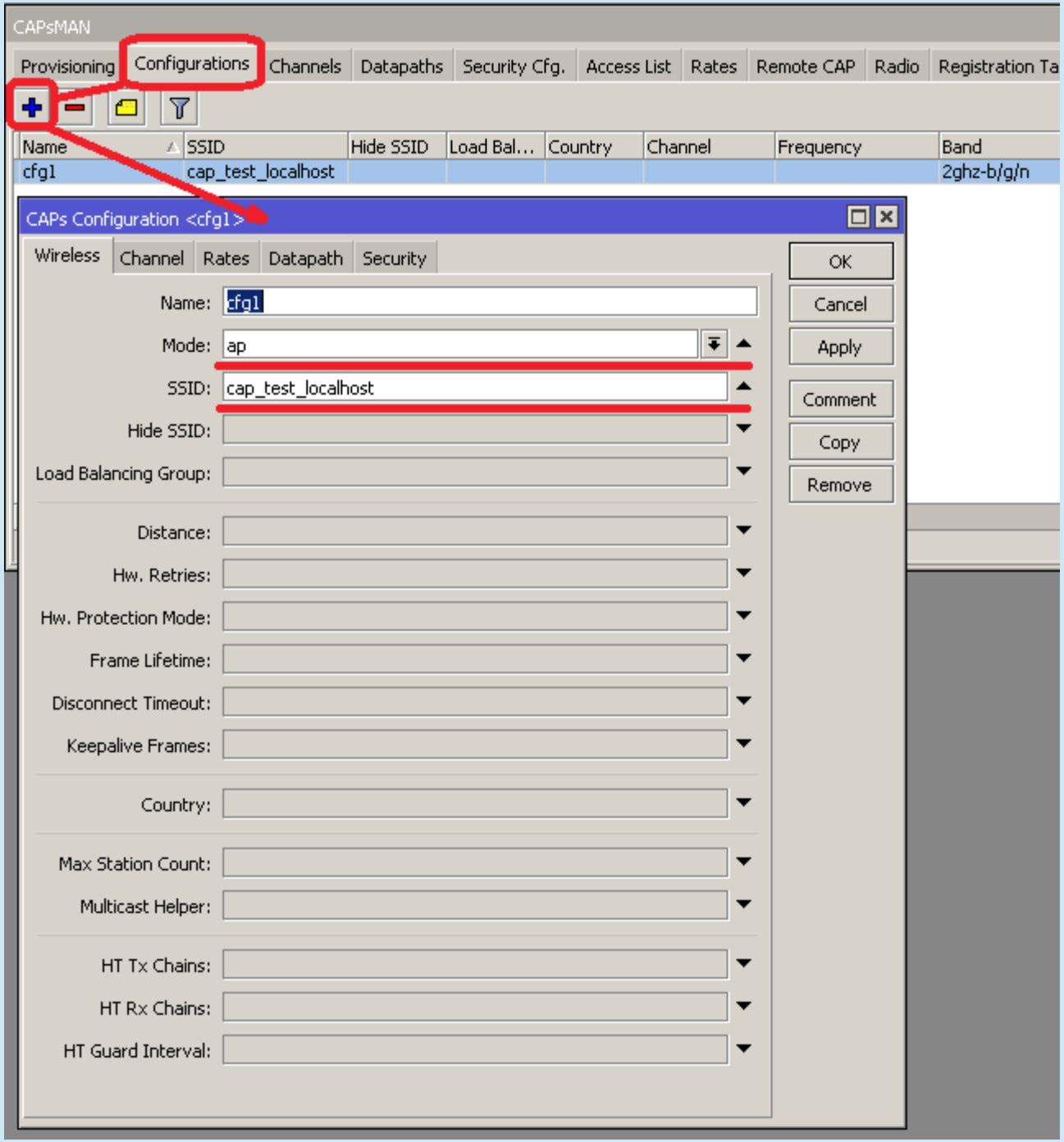
Oter parameters depending on configuration

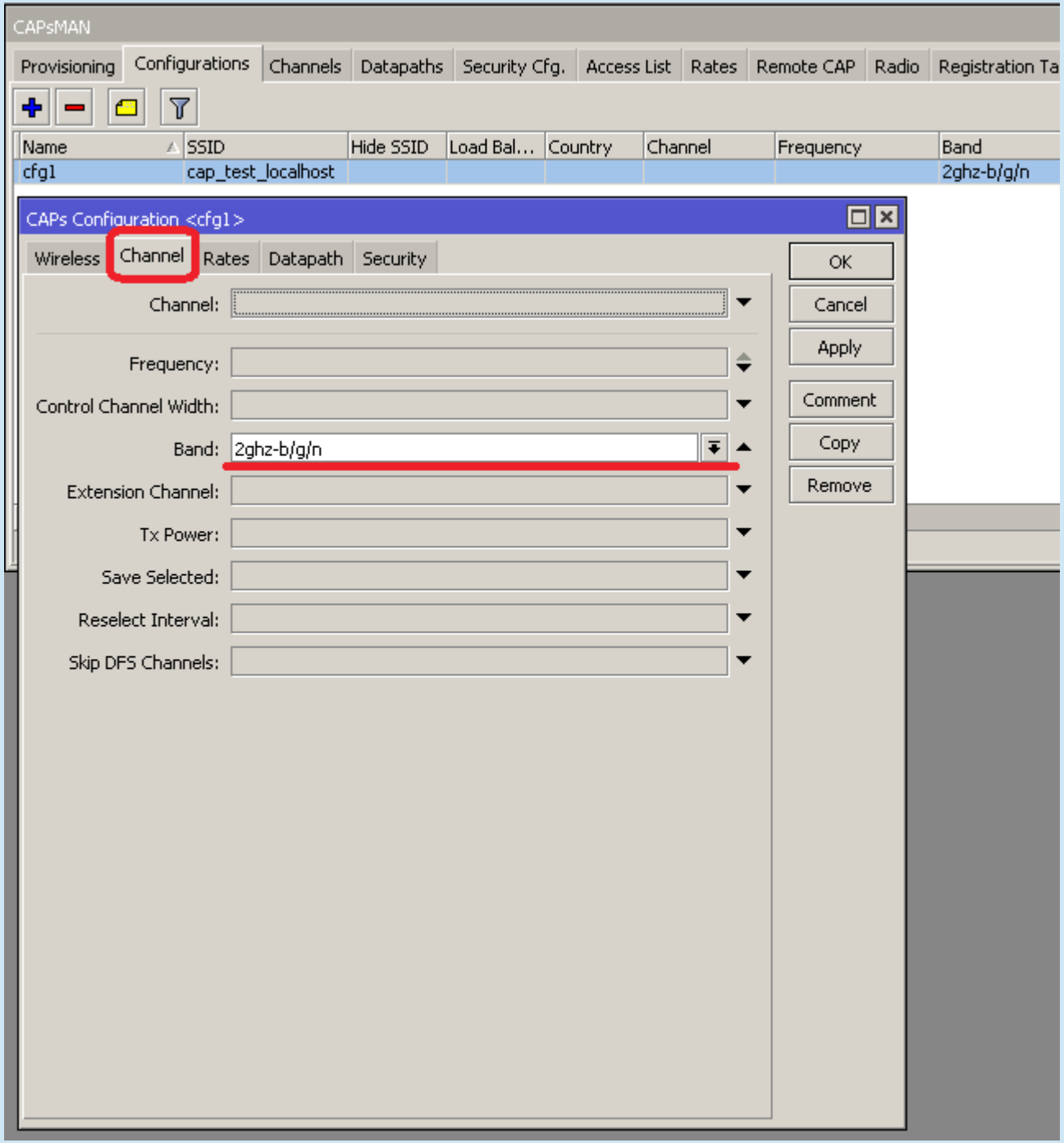
```
caps-man-addresses
discovery-interfaces
Bridge
```

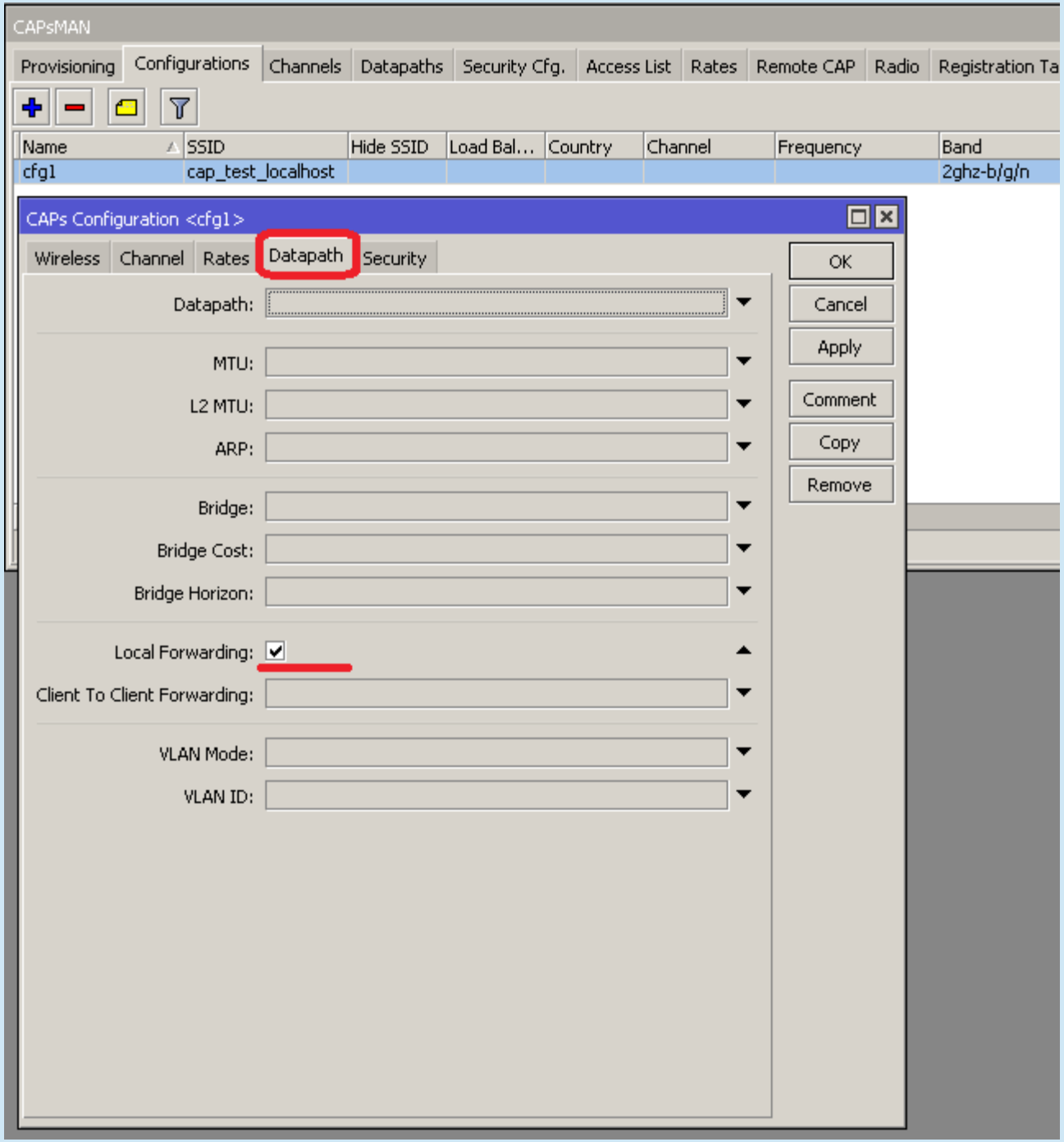
Default CAP configuration loaded by holding reset button for 10 seconds

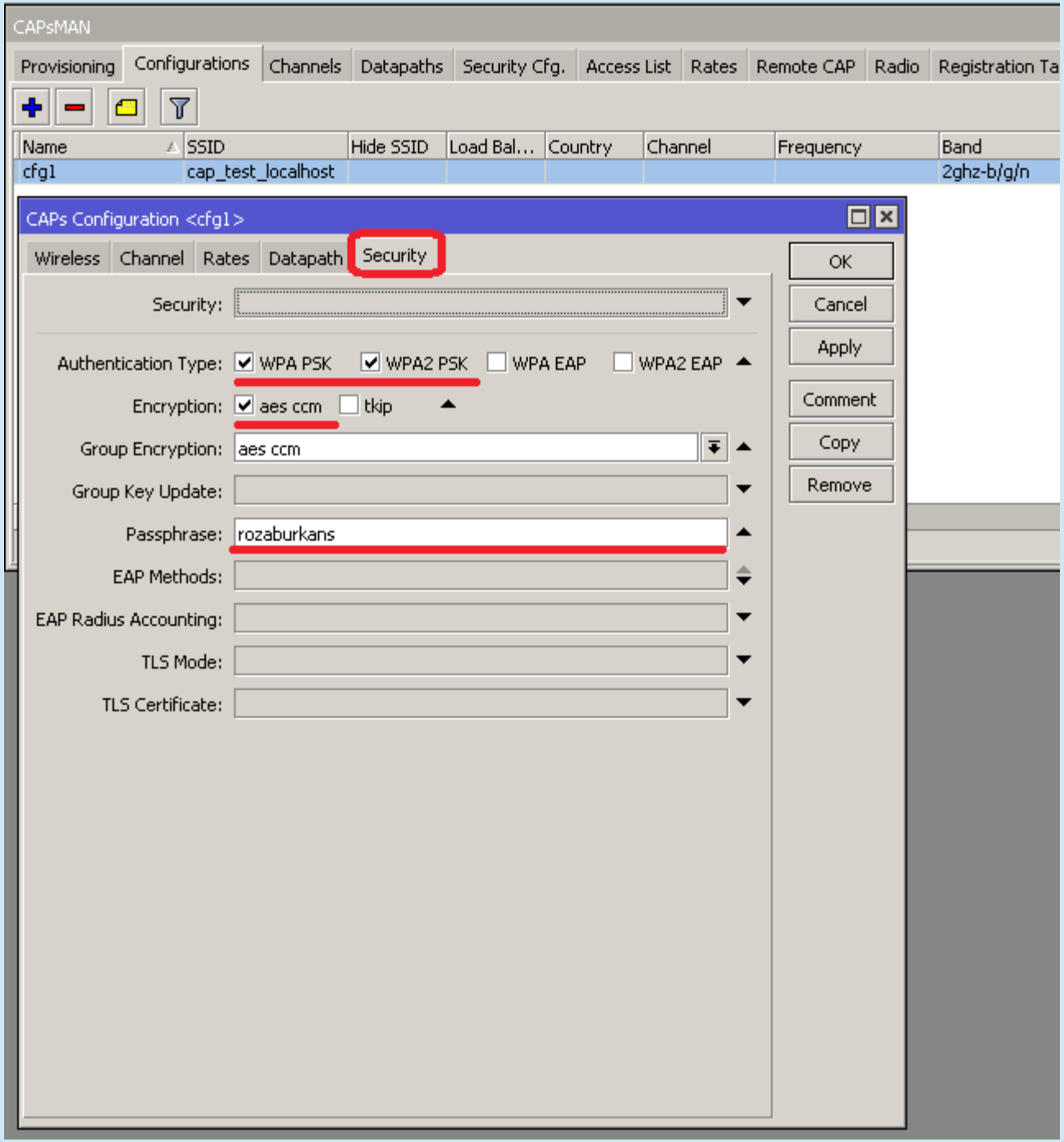
CAPsMAN

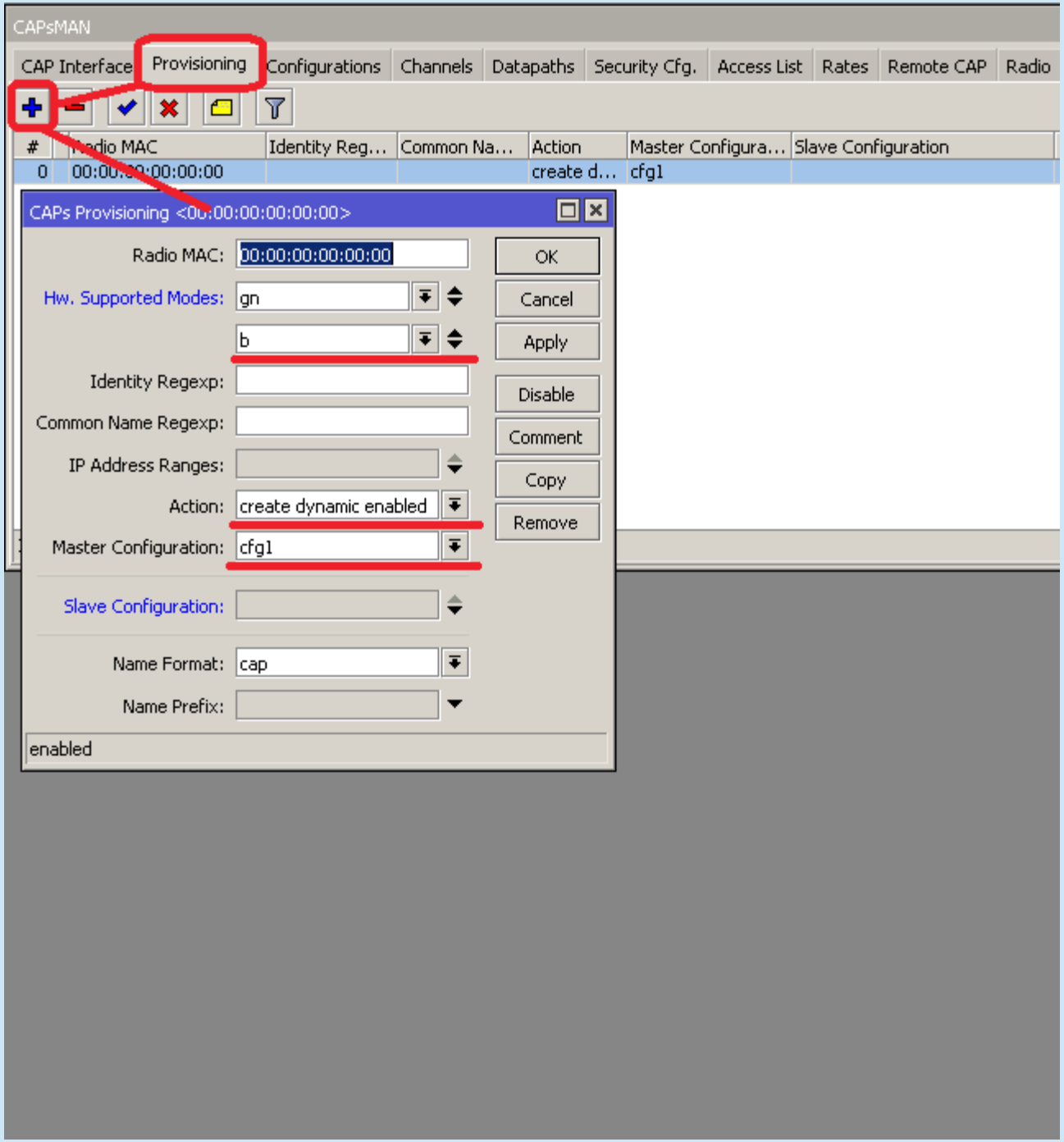
- CAP and CAPsMAN can be on the same router, set to 'loopback' or 127.0.0.1
- To provision configuration CAPsMAN needs:
  - To get connection from CAP and discover its interfaces
  - To have configuration parameters
  - To have provisioning criteria

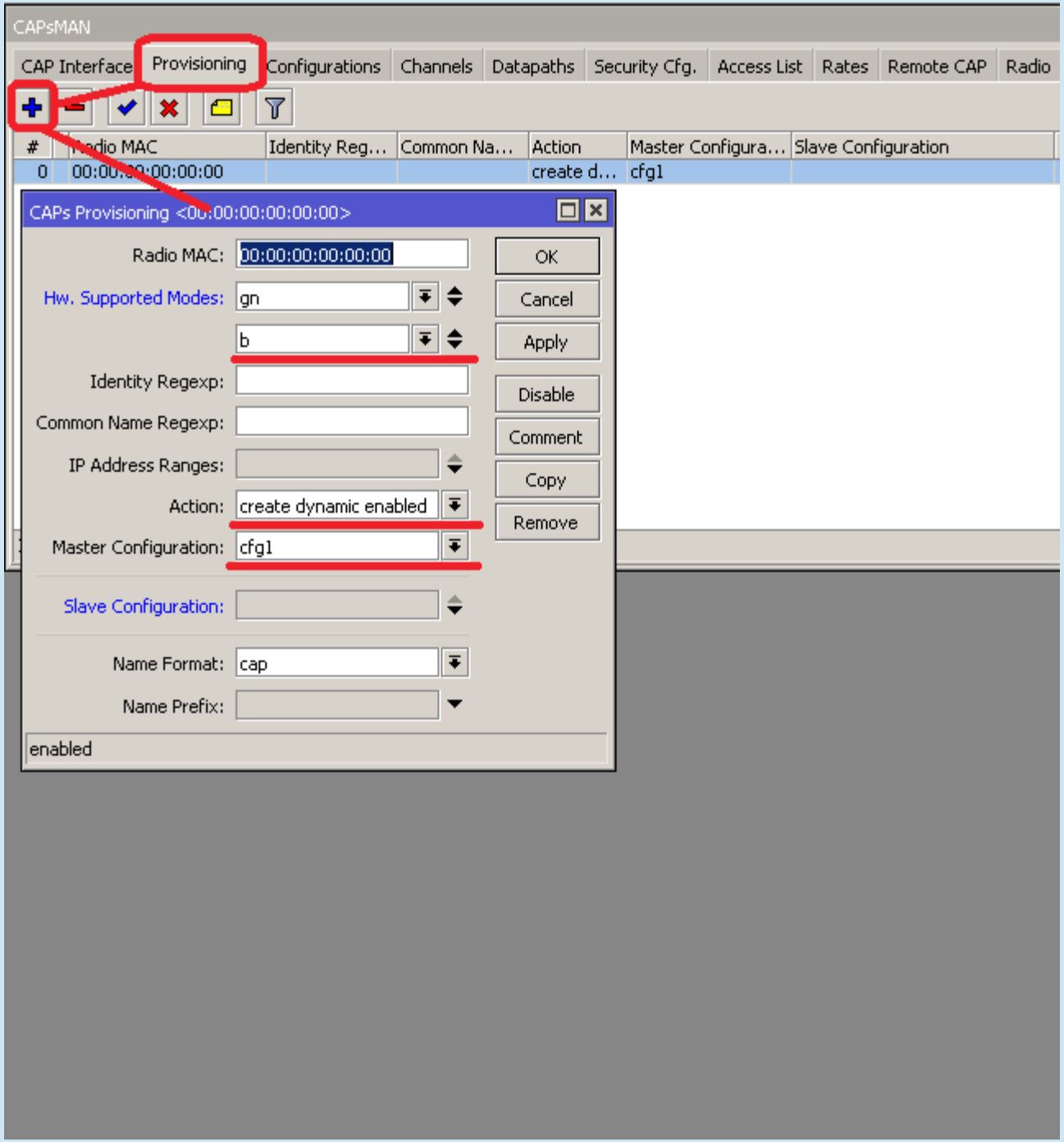

CAPsMAN
Provisioning
Configurations
Channels
Datapaths
Security Cfg.
Access List
Rates
Remote CAP
Radio
Registration Ta
Name
SSID
Hide SSID
Load Bal...
Country
Channel
Frequency
Band
cfg1
cap_test_localhost
2ghz-b/g/n
CAPs Configuration <cfg1>
Wireless
Channel
Rates
Datapath
Security
OK
Cancel
Apply
Comment
Copy
Remove
Name:
cfg1
Mode:
ap
SSID:
cap_test_localhost
Hide SSID:
Load Balancing Group:
Distance:
Hw. Retries:
Hw. Protection Mode:
Frame Lifetime:
Disconnect Timeout:
Keepalive Frames:
Country:
Max Station Count:
Multicast Helper:
HT Tx Chains:
HT Rx Chains:
HT Guard Interval:


CAPsMAN
Provisioning
Configurations
Channels
Datapaths
Security Cfg.
Access List
Rates
Remote CAP
Radio
Registration Ta
Name
SSID
Hide SSID
Load Bal...
Country
Channel
Frequency
Band
cfg1
cap_test_localhost
2ghz-b/g/n
CAPs Configuration <cfg1>
Wireless
Channel
Rates
Datapath
Security
OK
Cancel
Apply
Comment
Copy
Remove
Channel:
Frequency:
Control Channel Width:
Band:
2ghz-b/g/n
Extension Channel:
Tx Power:
Save Selected:
Reselect Interval:
Skip DFS Channels:

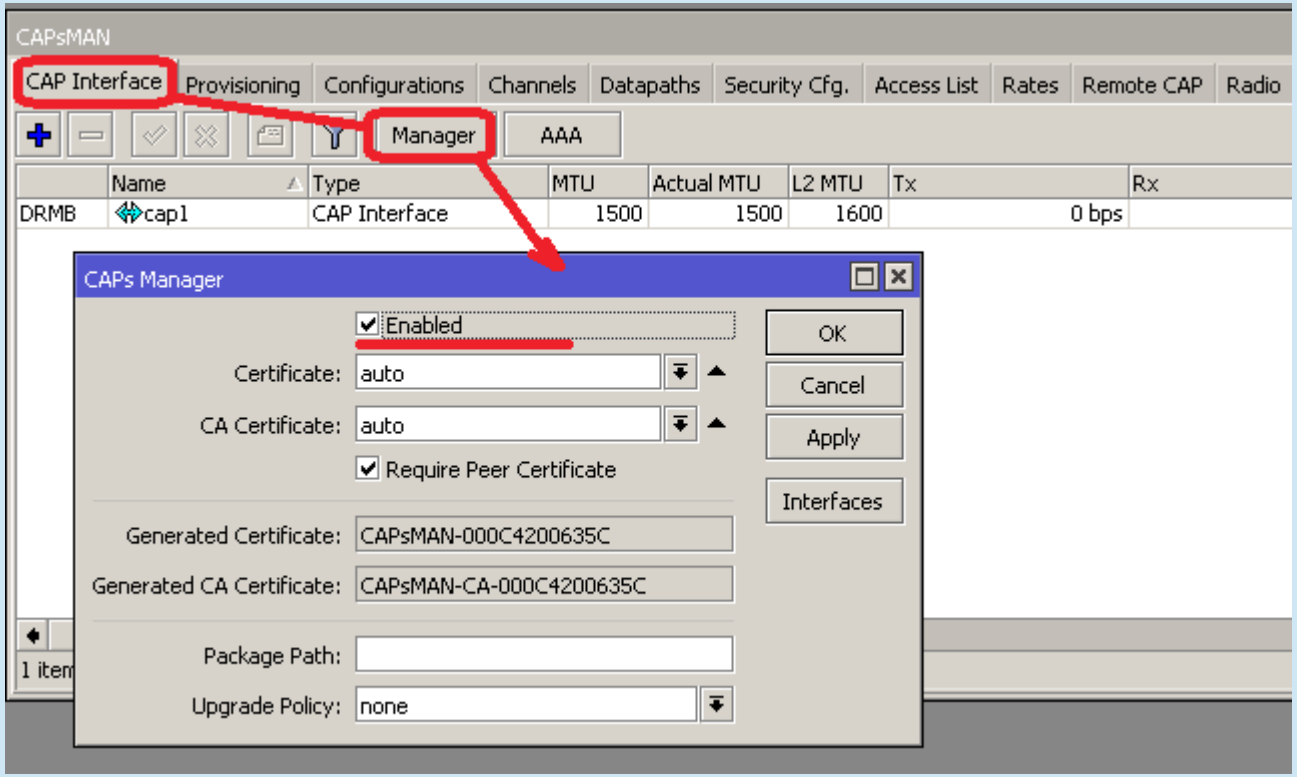

CAPsMAN
Provisioning
Configurations
Channels
Datapaths
Security Cfg.
Access List
Rates
Remote CAP
Radio
Registration Ta
Name
SSID
Hide SSID
Load Bal...
Country
Channel
Frequency
Band
cfg1
cap_test_localhost
2ghz-b/g/n
CAPs Configuration <cfg1>
Wireless
Channel
Rates
Datapath
Security
OK
Cancel
Apply
Comment
Copy
Remove
Datapath:
MTU:
L2 MTU:
ARP:
Bridge:
Bridge Cost:
Bridge Horizon:
Local Forwarding:
Client To Client Forwarding:
VLAN Mode:
VLAN ID:


CAPsMAN
Provisioning
Configurations
Channels
Datapaths
Security Cfg.
Access List
Rates
Remote CAP
Radio
Registration Ta
Name
SSID
Hide SSID
Load Bal...
Country
Channel
Frequency
Band
cfg1
cap_test_localhost
2ghz-b/g/n
CAPs Configuration <cfg1>
Wireless
Channel
Rates
Datapath
Security
OK
Cancel
Apply
Comment
Copy
Remove
Security:
Authentication Type:
WPA PSK
WPA2 PSK
WPA EAP
WPA2 EAP
Encryption:
aes ccm
tkip
Group Encryption:
aes ccm
Group Key Update:
Passphrase:
rozaburkans
EAP Methods:
EAP Radius Accounting:
TLS Mode:
TLS Certificate:

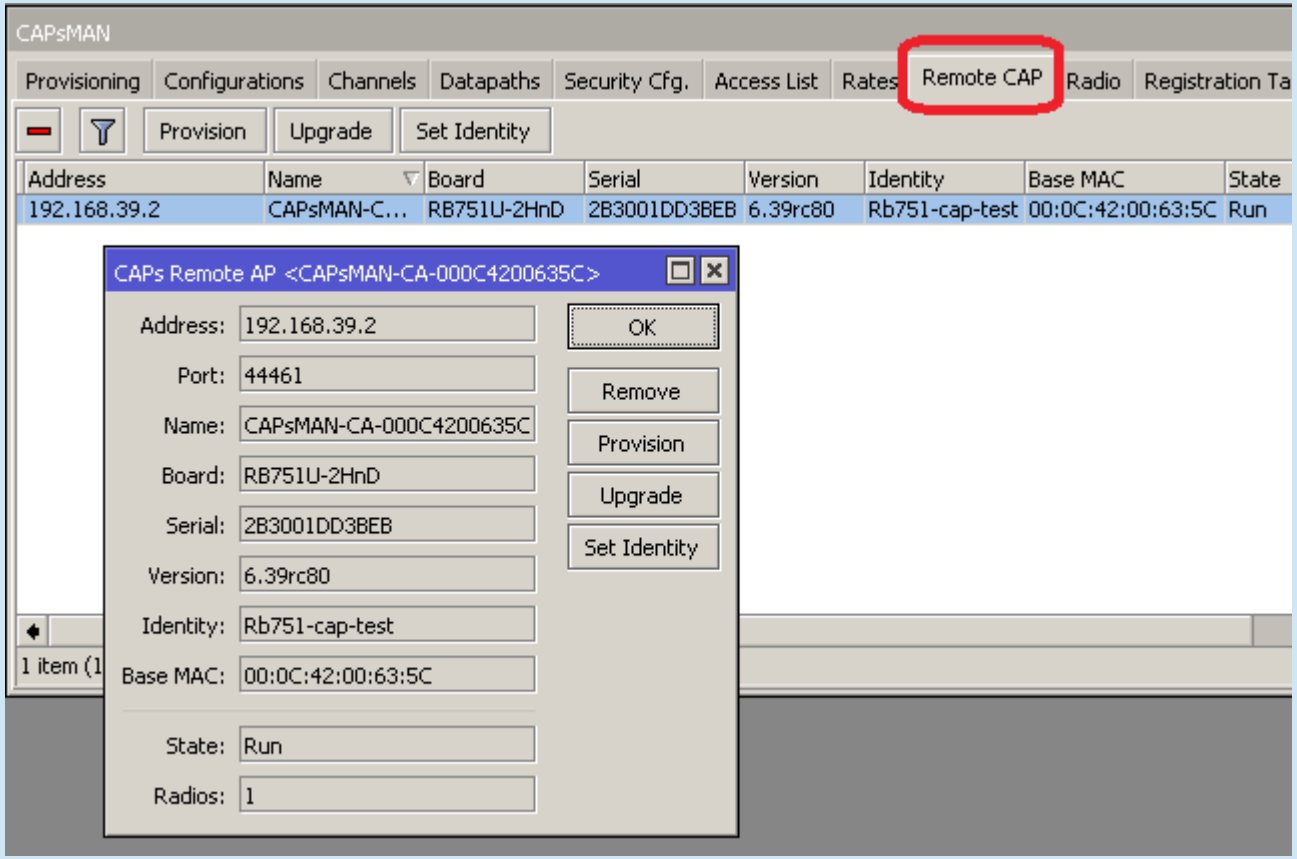

CAPsMAN
CAP Interface
Provisioning
Configurations
Channels
Datapaths
Security Cfg.
Access List
Rates
Remote CAP
Radio
| Radio MAC | Identity Reg... | Common Na... | Action | Master Configura... | Slave Configuration
0 | 00:00:00:00:00:00 | | | create d... | cfg1 |
CAPs Provisioning <00:00:00:00:00:00>
Radio MAC: 00:00:00:00:00:00
Hw. Supported Modes: gn
b
Identity Regexp:
Common Name Regexp:
IP Address Ranges:
Action: create dynamic enabled
Master Configuration: cfg1
Slave Configuration:
Name Format: cap
Name Prefix:
OK
Cancel
Apply
Disable
Comment
Copy
Remove
enabled


CAPsMAN
CAP Interface
Provisioning
Configurations
Channels
Datapaths
Security Cfg.
Access List
Rates
Remote CAP
Radio
| Radio MAC | Identity Reg... | Common Na... | Action | Master Configura... | Slave Configuration
0 | 00:00:00:00:00:00 | | | create d... | cfg1 |
CAPs Provisioning <00:00:00:00:00:00>
Radio MAC: 00:00:00:00:00:00
Hw. Supported Modes: gn
b
Identity Regexp:
Common Name Regexp:
IP Address Ranges:
Action: create dynamic enabled
Master Configuration: cfg1
Slave Configuration:
Name Format: cap
Name Prefix:
OK
Cancel
Apply
Disable
Comment
Copy
Remove
enabled

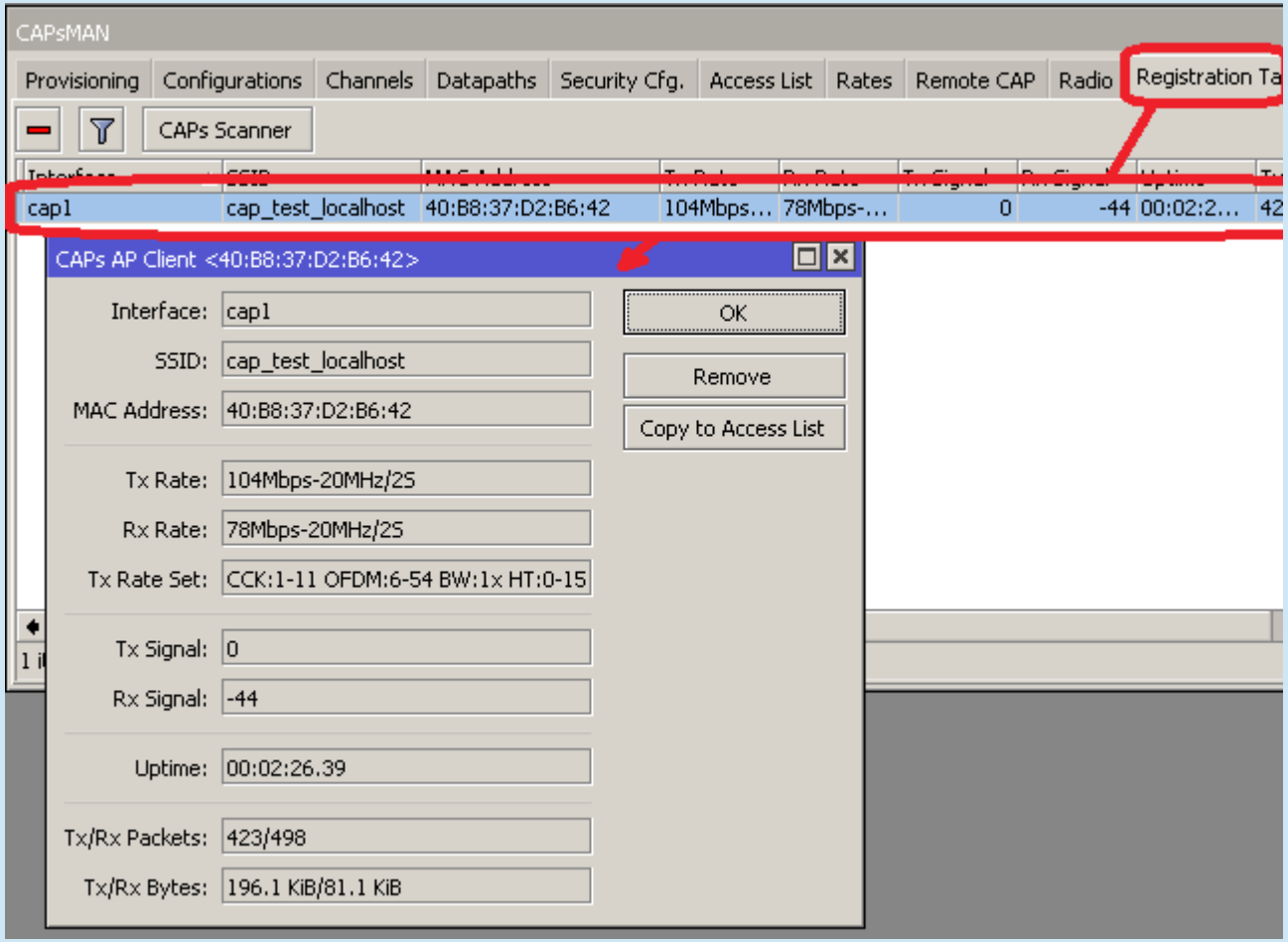
CAPsMAN


CAPsMAN
CAP Interface
Provisioning
Configurations
Channels
Datapaths
Security Cfg.
Access List
Rates
Remote CAP
Radio
Manager
AAA
Name
Type
MTU
Actual MTU
L2 MTU
Tx
Rx
DRMB
cap1
CAP Interface
1500
1500
1600
0 bps
CAPs Manager
Enabled
Certificate:
auto
CA Certificate:
auto
Require Peer Certificate
Generated Certificate:
CAPsMAN-000C4200635C
Generated CA Certificate:
CAPsMAN-CA-000C4200635C
Package Path:
Upgrade Policy:
none
OK
Cancel
Apply
Interfaces
1 item

CAPsMAN


CAPsMAN
Provisioning
Configurations
Channels
Datapaths
Security Cfg.
Access List
Rates
Remote CAP
Radio
Registration Ta
Provision
Upgrade
Set Identity
Address
Name
Board
Serial
Version
Identity
Base MAC
State
192.168.39.2
CAPsMAN-C...
RB751U-2HnD
2B3001DD3BEB
6.39rc80
Rb751-cap-test
00:0C:42:00:63:5C
Run
CAPs Remote AP <CAPsMAN-CA-000C4200635C>
Address: 192.168.39.2
Port: 44461
Name: CAPsMAN-CA-000C4200635C
Board: RB751U-2HnD
Serial: 2B3001DD3BEB
Version: 6.39rc80
Identity: Rb751-cap-test
Base MAC: 00:0C:42:00:63:5C
State: Run
Radios: 1
OK
Remove
Provision
Upgrade
Set Identity
1 item (1

CAPsMAN


CAPsMAN
Provisioning
Configurations
Channels
Datapaths
Security Cfg.
Access List
Rates
Remote CAP
Radio
Registration Ta
CAPs Scanner
cap1
cap_test_localhost
40:B8:37:D2:B6:42
104Mbps...
78Mbps-...
0
-44
00:02:2...
CAPs AP Client <40:B8:37:D2:B6:42>
Interface: cap1
SSID: cap_test_localhost
MAC Address: 40:B8:37:D2:B6:42
Tx Rate: 104Mbps-20MHz/2S
Rx Rate: 78Mbps-20MHz/2S
Tx Rate Set: CCK:1-11 OFDM:6-54 BW:1x HT:0-15
Tx Signal: 0
Rx Signal: -44
Uptime: 00:02:26.39
Tx/Rx Packets: 423/498
Tx/Rx Bytes: 196.1 KiB/81.1 KiB
OK
Remove
Copy to Access List

CAPsMAN

- Possibility to provision different configurations on the same device (2GHz and 5GHz)
  - Create two configurations
  - Create two provisioning criteria (bgn, an or ac)
- Common config parameters can be set in templates (channel, datapath, security)

CAPsMAN Limitations

- 32 Radios per CAP
- 32 Virtual interfaces per master radio interface
- But unlimited CAPs (access points) supported by CAPsMAN
- CAPsMAN v1 not compatible with v2
- No Nstreme, NV2 support

Thank you!